Amendments to the Claims:

The following listing of the claims replaces all previous listings and versions of the claims in the application:

Listing of the Claims:

Claims 1-19: (Cancelled)

20. (Currently Amended) A method of establishing a communication path in a data communication network from a chip card associated with a client, comprising the steps of:

providing a privacy reference point in said data communication network, said privacy reference point configured for use in one transaction, said privacy reference point identified by a domain offset link and a relative reference;

establishing a first communication path from said chip card to said privacy reference point;

providing an authentication of said chip card relative to said privacy reference point;

verifying the authentication of said chip card relative to said privacy reference point from said chip card; and

establishing a second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network;

wherein at least one of the steps of verifying the authentication and establishing a second communication path is performed without disclosing the identity of said chip card.

21. (Previously Presented) The method according to claim 20, wherein the step of providing an authentication comprises the steps of:

registering data selected from the group consisting of biometrics, a signature, a code, and any combinations thereof; and

comparing the registered data with corresponding stored data.

2

22. (Previously Presented) The method of claim 20, wherein the step of verifying the authentication is performed without disclosing the identity of said chip card.

23. (Previously Presented) The method of claim 20, wherein the step of establishing a second communication path is performed without disclosing the identity of said chip card.

24. (Previously Presented) The method according to either of claims 20 or 21, wherein said chip card includes encrypted data, said method further comprising:

said chip card receiving an encrypted key from said privacy reference point;

decrypting said encrypted key using a second stored key to create a decrypted version of the encrypted key; and

decrypting said encrypted data using the decrypted version of said encrypted key.

25. (Previously Presented) The method according to either of claims 20 or 21, said communication network being selected from a group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

26. (Previously Presented) The method according to either of claims 20 or 21, said chip card having an authenticated holder, and said privacy reference point being addressable by the authenticated holder from a computer communicating with said data communication network.

27. (Previously Presented) The method according to either of claims 20 or 21, further comprising said chip card allowing or blocking access to said privacy reference point by a second communication device.

28. (Cancelled)

29. (Previously Presented) The method according to either of claims 20 or 21, wherein at least one of said steps of establishing a first communication path and establishing a second communication path involves creating and negotiating an accountability path adapted to a context risk profile.

30. (Previously Presented) The method according to claim 29, wherein said chip card has an authenticated holder, and said first communication device establishes a procedure to identify a party selected from a group consisting of said chip card and the authenticated holder of said chip card.

31. (Previously Presented) The method according to claim 30, wherein said procedure to identify a party employs identification information selected from a group consisting of at least one of biometrics, name, digital signature, and a code.

32. (Previously Presented) The method according to either of claims 20 or 21, further comprising:

> providing an identity provider and a service provider;

> establishing communication from said first communication device to said service provider;

> establishing communication from said service provider to said identity provider;

> providing a further communication device associated with a financial institution;

> establishing communication from said service provider to said further communication device;

> transmitting information from said first communication device to said service provider;

> transmitting said information from said service provider to said identity provider;

> transmitting said information from said identity provider to said further communication device;

> said further communication device responding to said information by transmitting a payment acceptance to said identity provider;

> said identity provider transmitting said payment acceptance to said service provider; and

said service provider transmitting said payment acceptance to said first communication device.

33-39. (Cancelled)

40. (New) A method of establishing a communication path through a communication network between a first device and a second device,

wherein the first device and the second device are able to communicate without any other device in the communication network being able to distinguish between two transactions between the first device and the second device and two transactions between any other two devices in the communication network;

wherein the first device and the second device independently connect to a same connection address in an address space hosted in the communication network without reusing any identifier related to the first device or the second device; and

wherein the connection address is generated using a first algorithm.

41. (New) The method of claim 40, wherein the algorithm consists of an absolute offset and a relative address component combined to form the connection address;

wherein the absolute offset is either an address in the address space, an address of the first device, or an address of the second device;

wherein the relative address component is created using a second algorithm having as an input a shared secret combined with an element selected from the group consisting of a next unused in a pre-shared list of one-time-only keys, a time-dependent component, a counter changing with each session, a command-specific component, a group-specific component, an event-specific component, a salt, and combinations thereof; and

wherein the second algorithm is a first one-way mathematical function.

42. (New) The method of claim 41, wherein the relative address component is used to create an authentication specific of the first device as a requesting device to the second device as a verifying device;

wherein the relative address component is used as key to encrypt a random session key generated by the requesting device;

wherein the method comprises:

providing a message authentication component derived from a second one-way mathematical function using as an input a combination of the shared secret, the random session key, and the element input to the second algorithm;

forwarding the message authentication component to the verifying device through the communication network using the communication path;

recreating, in the verifying device, the relative address component using the forwarded message authentication component as a decryption key to receive the random session key;

using the random session key to decrypt and derive forwarded parameter data; and

validating, in the verifying device, the forwarded message authentication component to derive an expected message authentication component.

43. (New) The method of claim 42, further comprising responding with a response selected from the group consisting of remaining silent, a random identifier, a next item in a list of one-time-only identifiers, a return authentication message component derived using a third one-way mathematical function, and a combination of the shared secret, the random session secret, and the element used in the second algorithm.